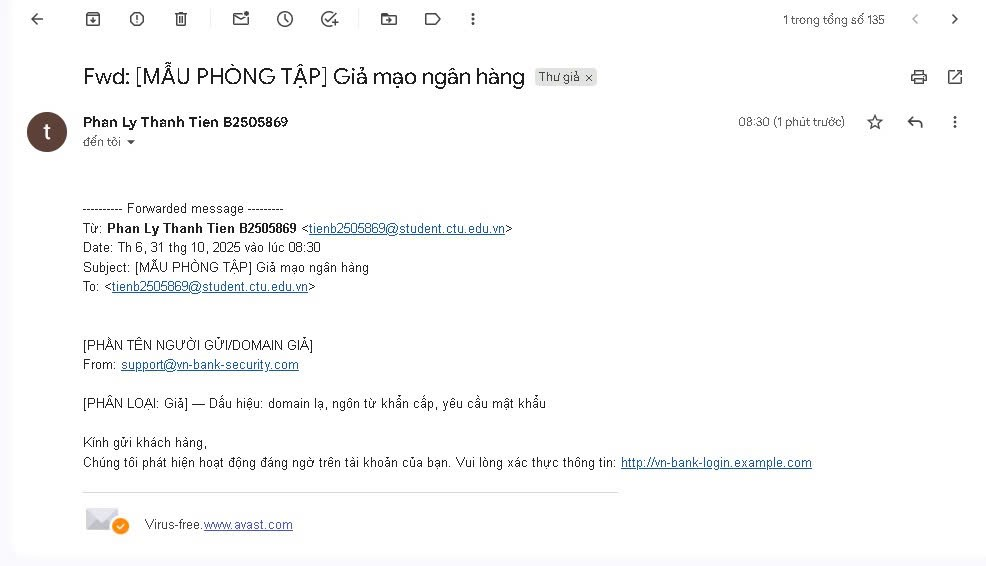
TIẾT 4

Phân loại 5 email sao:



* Email giả:

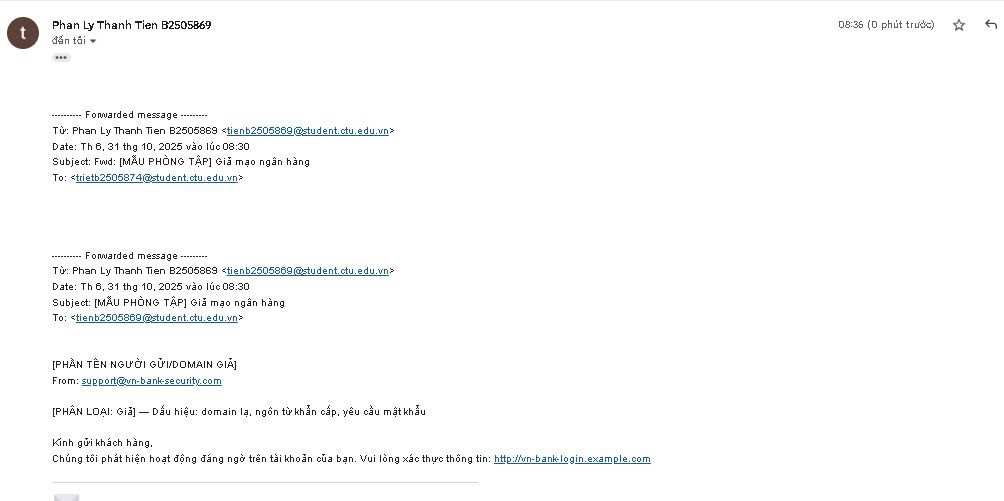


Lí do: Đây là thư giả vì domain người gửi không chính thức (vn-bank-security.com), link dẫn tới trang lạ (.example) yêu cầu nhập thông tin nhạy cảm, dùng ngôn ngữ khẩn cấp và lời chào chung chung, không cá nhân hoá. Email thiếu chữ ký và thông tin xác thực của ngân hàng, dấu hiệu rõ ràng của phishing.



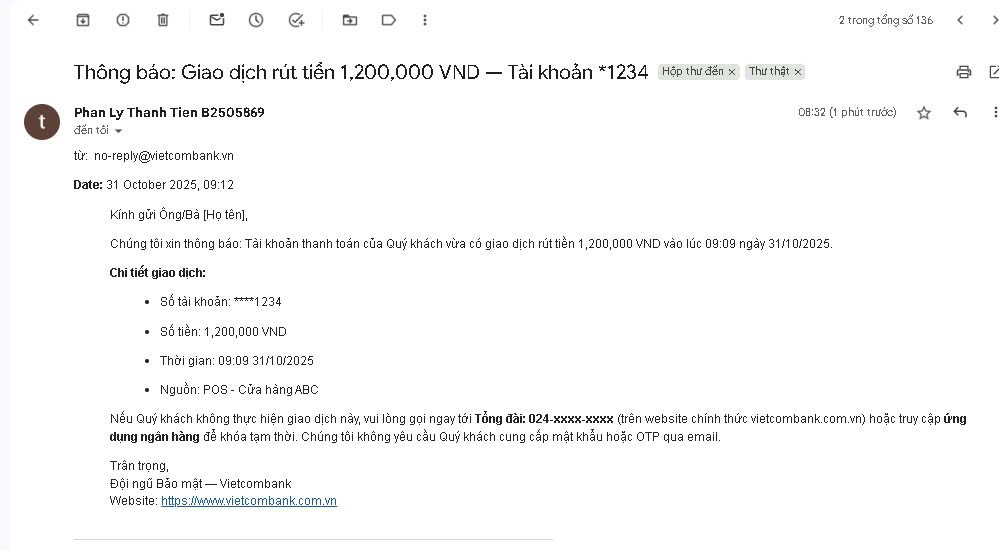
Lí Do:

* Sender không thuộc domain chính thức (promo@techstore-vip.com)
* Link dẫn tới domain giả (facebook-check.example)
* Yêu cầu đăng nhập qua link lạ → nguy cơ phishing
* Ngôn ngữ khẩn cấp, tạo áp lực
* Thiếu chữ ký và thông tin xác thực của Facebook
* Hành động: không bấm link, báo cáo phishing, xóa email



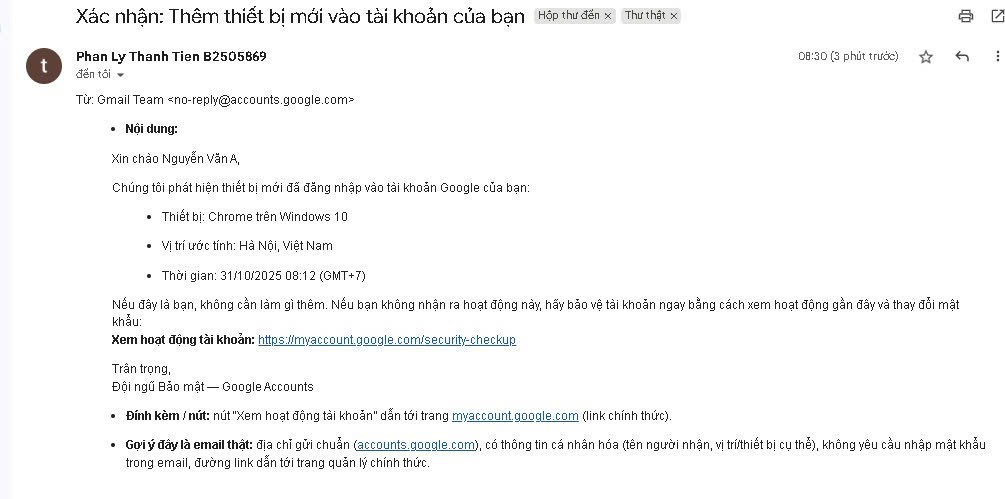
Lí do: domain lạ, ngôn từ khẩn cấp, yêu cầu mật khẩu

* Email thật:



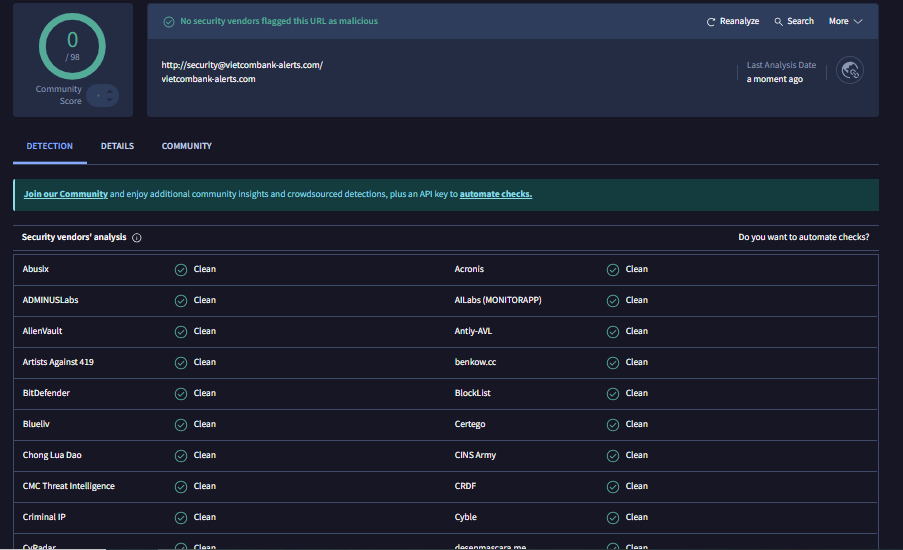
Lí do:

* Sender thuộc domain chính thức (no-reply@vietcombank.vn)
* Chứa thông tin cá nhân hoá (tên, 4 số cuối tài khoản)
* Nội dung chi tiết, hợp lý về giao dịch, không yêu cầu mật khẩu/OTP
* Có chữ ký, số tổng đài và link tới website chính thức của ngân hàng
* Ngôn từ chuyên nghiệp, không tạo áp lực khẩn cấp giả tạo



Lí do:

* Sender thuộc domain chính thức (no-reply@accounts.google.com)
* Chứa thông tin cá nhân hoá (tên, thiết bị, vị trí đăng nhập)
* Link dẫn tới trang quản lý Google chính thức (myaccount.google.com)
* Không yêu cầu nhập mật khẩu trực tiếp trong email
* Ngôn từ chuyên nghiệp, có chữ ký đội ngũ Bảo mật Google
* kiểm tra đường link bằng VirusTotal.



Báo cáo: 5 dấu hiệu nhận biết email/website lừa đảo

* Người gửi không đáng tin / tên miền lạ
* Yêu cầu hành động khẩn cấp hoặc đe dọa
* Link/URL bất thường khi di chuột
* Đính kèm khả nghi hoặc định dạng nguy hiểm
* Ngôn ngữ, chính tả, cấu trúc lạ

Hành động đề xuất:

* Không click link hoặc mở file nghi ngờ
* Kiểm tra link bằng VirusTotal / Google Safe Browsing
* Báo cho CNTT / giảng viên nếu nghi ngờ
* Đổi mật khẩu và bật xác minh 2 bước nếu cần